**Summary of Anderson’s Paper**

**INTRODUCTION**:

We are going to see the insight of the PUF’s design in this paper. We define the FPGA architecture for the secure PUF design for various applications such as digital rights management, IP Protection, cryptographic key generation, device authentication and IC counterfeit detection prevention.

Four main categories of PUF are:

1) Ring oscillator based PUF

2)Arbiter PUF

3) Memory based PUF- It uses the random initial state of memory bits on device start up as the PUF signature.

4) glitch count based PUF- counts variability dependant glitches on the output of a combinational multiplier.

XILINX VIRTEX-5 FPGA:

**Virtex-5 Logic Block**:

Virtex-5 logic Block is called a CLB and each CLB consists of two SLICES. A SLICE contains four 6 input lookup table, four flip flops and arithmetic circuitry. Each LUT has a RAM cell that hold the truth table of the logic function implemented by the LUT. The LUT output is connected to the select line of the 2 to 1 multiplexer. Each 6 LUT has 64 SRAM cells and can be used as 64\*1 SRAM cell.

**PUF DESIGN**:

We have two LUT’s that generate the opposite patterns of sequence such that as follows.

LUT A:0101010010101010(0\*5555)

LUT B:1010101010101010(0\*AAAA)

A close up of text on a white background

Description generated with very high confidence

These are the initial values for the LUT’s. The IN pin makes sure that this pattern continues every 16 cycles for the 2 LUT’s and the OUT pins are used to drive the select input pins on carry chain multiplexers. Both carry multiplexer have their ‘0’ input tied to logic-0 and the bottom carry chain multiplexer has ‘1’ data input tied to logic-1.

Consider the initial case LUTA is at logic-0 so we get N2 at logic-0. The output pin of LUT B is 1. At rising edge, the OUTPUT pin of LUTA will change from logic-0 to logic-1 and the output pin of LUT B will change from logic-1 to logic-0. Although LUT A and the multiplexer it drives as same as the LUT B, the two pieces of circuitry in fact experience different delays due to random process variations.

We have two cases to look upon. First case when LUT B and the multiplexer is faster than LUT A and its multiplexer. In this case, LUT B transitions from logic 1 to 0, similarly N1 also transitions from logic 1 to 0. Following that slower LUT A transitions from logic 0 to 1,such that signal N2 is kept constant at logic 0 throughout the process. The second case is the opposite one where LUT A and its multiplexer is faster than LUT B and its multiplexer. In this case, LUT A ‘s OUT pin transitions from logic 0 to 1 and net N1 has not yet transitioned from logic 1 to logic 0. Therefore, we have a short positive spike(glitch) will appear on N2 for the period before N1 transitions to logic-0. The presence or absence of a positive spike on N2 and the length of the spike pulse, are due to the process variations that impact LUT A and LUT B. This variation in N2 is used to determine the PUF signature bit. Whenever there is a glitch we get a logic-1, otherwise it’s at logic 0. If the pulse is always generated and its width is too wide ,it’s more likely to reach the flipflop preset input, making PUF bit 1.

we need to keep in mind that the pulse width is more to create a good PUF design. For this, we have make LUT B as far as it can so that we get a longer pulse width to be produced within the proposed PUF design.

A screenshot of a cell phone

Description generated with very high confidence

Therefore, we form a challenge/response network. Usually, the challenge selects two different PUF bits to produce whose values are xor’ed to produce an output bit depending on the challenge.

**EXPERIMENTAL VALIDATION**:

The same circuit is instantiated 128 times to generate a 128-bit signature. We found that signatures between chips at different regions is unique. With 6 PUF’s per chip ad 6 chips in total, we will have 36 PUF implementations. As there are 6 PUF’s on each FPGA we can compute (6\*5)/2=15 data points for each chip getting a total of 6\*15=90 data points in total. On average the distance between signature was 59 which is close to the expected value 64.